Codes Associated with $O^+(2n, 2^r)$ and Power Moments of Kloosterman Sums

Dae San Kim, *Member, IEEE*

***Abstract*— In this paper, we construct three binary linear codes $C(SO^+(2,q))$, $C(O^+(2,q))$, $C(SO^+(4,q))$, respectively associated with the orthogonal groups $SO^+(2,q)$, $O^+(2,q)$, $SO^+(4,q)$, with q powers of two. Then we obtain recursive formulas for the power moments of Kloosterman and 2-dimensional Kloosterman sums in terms of the frequencies of weights in the codes. This is done via Pless power moment identity and by utilizing the explicit expressions of Gauss sums for the orthogonal groups. We emphasize that, when the recursive formulas for the power moments of Kloosterman sums are compared, the present one is computationally more effective than the previous one constructed from the special linear group $SL(2,q)$. We illustrate our results with some examples.**

***Index Terms*— Kloosterman sum, 2-dimensional Kloosterman sum, orthogonal group, Pless power moment identity, weight distribution, Gauss sum.**

I. Introduction

Let ψ be a nontrivial additive character of the finite field $\mathbb{F}_q$ with $q = p^r$ elements (p a prime), and let m be a positive integer. Then the m-dimensional Kloosterman sum $K_m(\psi; a)$([11]) is defined by

$$K_m(\psi; a) = \sum_{\alpha_1,\cdots,\alpha_m \in \mathbb{F}_q^*} \psi(\alpha_1 + \cdots + \alpha_m + a\alpha_1^{-1}\cdots\alpha_m^{-1}) \qquad (a \in \mathbb{F}_q^*).$$

In particular, if $m = 1$, then $K_1(\psi; a)$ is simply denoted by $K(\psi; a)$, and is called the Kloosterman sum. The Kloosterman sum was introduced in 1926 ([9]) to give an estimate for the Fourier coefficients of modular forms.

For each nonnegative integer h, by $MK_m(\psi)^h$ we will denote the h-th moment of the m-dimensional Kloosterman sum $K_m(\psi; a)$. Namely, it is given by

$$MK_m(\psi)^h = \sum_{a \in \mathbb{F}_q^*} K_m(\psi; a)^h.$$

If $\psi = \lambda$ is the canonical additive character of $\mathbb{F}_q$, then $MK_m(\lambda)^h$ will be simply denoted by MK_m^h. If further $m = 1$, for brevity MK_1^h will be indicated by MK^h. The power moments of Kloosterman sums can be used, for example, to give an estimate for the Kloosterman sums and have also been studied to solve a variety of problems in coding theory over finite fields of characteristic two.

From now on, let us assume that $q = 2^r$. Carlitz [1] evaluated MK^h, for $h \le 4$, while Moisio [16] computed it for $h = 6$. Recently, Moisio was able to find explicit expressions of MK^h, for the other values of h for $h \le 10$ (cf. [13])(Similar results exist also over the finite fields of characteristic three (cf. [4],[14])). This was done, via Pless power moment identity, by connecting moments of Kloosterman sums and the frequencies of weights in the binary Zetterberg code of length $q+1$, which were known by the work of Schoof and Vlugt in [18]. In [7], the binary linear codes $C(SL(n,q))$ associated with finite special linear groups $SL(n,q)$ were constructed when n, q are both powers of two. Then obtained was a recursive formula for the power moments of multi-dimensional Kloosterman sums in terms of the frequencies of weights in $C(SL(n,q))$. This was done via Pless power moment identity and by utilizing our previous result on the explicit expression of the Gauss sum for $SL(n,q)$. In particular, when $n = 2$, this gives a recursive formula for the power moments of Kloosterman sums.

In this paper, we will show the following theorem giving recursive formulas for the power moments of Kloosterman and 2-dimensional Kloosterman sums. To do that, we construct three binary linear codes $C(SO^+(2,q))$, $C(O^+(2,q))$, $C(SO^+(4,q))$, respectively associated with $SO^+(2,q)$, $O^+(2,q)$, $SO^+(4,q)$, and express those power moments in terms of the frequencies of weights in each code. Then, thanks to our previous results on the explicit expressions of "Gauss sums" for the orthogonal group $O^+(2n,q)$ and the special orthogonal group $SO^+(2n,q)$ [8], we can express the weight of each codeword in the duals of the codes in terms of Kloosterman or 2-dimensional Kloosterman sums. Then our formulas will follow immediately from the Pless power moment identity.

The recursive formula for power moments of Kloosterman sums in this paper (cf. (1), (2)) is computationally more effective than that in [7](cf. [7], (3)). This is because it is easier to compute the weight distribution of $C(SO^+(2,q))$ than that of $C(SL(2,q))$. Theorem 1 in the following is the main result of this paper.

Theorem 1: Let $q = 2^r$. Then we have the following.

(a) For $r \ge 3$, and $h = 1, 2, \ldots,$

$$MK^h = \sum_{l=0}^{h-1} (-1)^{h+l+1} \binom{h}{l} (q-1)^{h-l} MK^l + q \sum_{j=0}^{min\{N_1,h\}} (-1)^{h+j} C_{1,j} \sum_{t=j}^{h} t! S(h,t) 2^{h-t} \binom{N_1 - j}{N_1 - t}, \tag{1}$$

where $N_1 = \mid SO^+(2,q) \mid = q-1$, and $\{C_{1,j}\}_{j=0}^{N_1}$ is the weight

The author is with the Department of Mathematics, Sogang University, Seoul 121-742, Korea(e-mail; dskim@sogang.ac.kr).

distribution of $C(SO^+(2,q))$ given by

$$C_{1,j} = \sum \binom{1}{\nu_0} \prod_{tr(\beta^{-1})=0} \binom{2}{\nu_\beta} (j = 0, \ldots, N_1). \quad (2)$$

Here the sum is over all the sets of nonnegative integers $\{\nu_0\} \bigcup \{\nu_\beta\}_{tr(\beta^{-1})=0}$ satisfying $\nu_0 + \sum_{tr(\beta^{-1})=0} \nu_\beta = j$ and $\sum_{tr(\beta^{-1})=0} \nu_\beta \beta = 0$. In addition, $S(h,t)$ is the Stirling number of the second kind defined by

$$S(h,t) = \frac{1}{t!} \sum_{j=0}^{t} (-1)^{t-j} \binom{t}{j} j^h. \quad (3)$$

(b) For $r \geq 3$, and $h = 1, 2, \ldots,$

$$MK^h = \sum_{l=0}^{h-1} (-1)^{h+l+1} \binom{h}{l} (q-1)^{h-l} MK^l + q \sum_{j=0}^{min\{N_2,h\}} (-1)^{h+j} C_{2,j} \sum_{t=j}^{h} t! S(h,t) 2^{h-t} \binom{N_2 - j}{N_2 - t}, \quad (4)$$

where $N_2 = \mid O^+(2,q) \mid = 2(q-1)$, and $\{C_{2,j}\}_{j=0}^{N_2}$ is the weight distribution of $C(O^+(2,q)$ given by

$$C_{2,j} = \sum \binom{q}{\nu_0} \prod_{tr(\beta^{-1})=0} \binom{2}{\nu_\beta} (j = 0, \ldots, N_2). \quad (5)$$

Here the sum is over all the sets of nonnegative integers $\{\nu_0\} \bigcup \{\nu_\beta\}_{tr(\beta^{-1})=0}$ satisfying $\nu_0 + \sum_{tr(\beta^{-1})=0} \nu_\beta = j$ and $\sum_{tr(\beta^{-1})=0} \nu_\beta \beta = 0$.

(c) For $r \geq 2$, and $h = 1, 2, \ldots,$

$$MK_2^h = \sum_{l=0}^{h-1} (-1)^{h+l+1} \binom{h}{l} (q^4 - q^3 - 2q^2 + 1)^{h-l} MK_2^l + q^{1-2h} \sum_{j=0}^{min\{N_3,h\}} (-1)^{h+j} C_{3,j} \sum_{t=j}^{h} t! S(h,t) 2^{h-t} \binom{N_3 - j}{N_3 - t}, \quad (6)$$

$$MK^{2h} = \sum_{l=0}^{h-1} (-1)^{h+l+1} \binom{h}{l} (q^4 - q^3 - 2q^2 + q + 1)^{h-l} MK^{2l} + q^{1-2h} \sum_{j=0}^{min\{N_3,h\}} (-1)^{h+j} C_{3,j} \sum_{t=j}^{h} t! S(h,t) 2^{h-t} \binom{N_3 - j}{N_3 - t}, \quad (7)$$

where $N_3 = \mid SO^+(4,q) \mid = q^2(q^2-1)^2$, and $\{C_{3,j}\}_{j=0}^{N_3}$ is the weight distribution of $C(SO^+(4,q))$ given by

$$C_{3,j} = \sum \binom{m_0}{\nu_0} \prod_{\substack{|t|<2\sqrt{q} \\ t \equiv -1(4)}} \prod_{K(\lambda;\beta^{-1})=t} \binom{m_t}{\nu_\beta} (j = 0, \ldots, N_3). \quad (8)$$

Here the sum is over all the sets of nonnegative integers $\{\nu_\beta\}_{\beta \in \mathbb{F}_q}$ satisfying $\sum_{\beta \in \mathbb{F}_q} \nu_\beta = j$ and $\sum_{\beta \in \mathbb{F}_q} \nu_\beta \beta = 0$,

$$m_0 = q^3(2q^2 - q - 2),$$

and

$$m_t = q^2(q^3 - q^2 - 2q + t),$$

for all integers t satisfying $|t| < 2\sqrt{q}$, and $t \equiv -1 \ (mod\ 4)$.

II. $O^+(2n,q)$

For more details about the results of this section, one is referred to the paper [8]. In addition, [19] is an excellent reference for matrix groups over finite fields.

Throughout this paper, the following notations will be used:

$q = 2^r$ ($r \in \mathbb{Z}_{>0}$),

$\mathbb{F}_q$ = the finite field with q elements,

TrA = the trace of A for a square matrix A,

${}^tB$ = the transpose of B for any matrix B.

Let θ^+ be the nondegenerate quadratic form on the vector space $\mathbb{F}_q^{2n\times 1}$ of all $2n \times 1$ column vectors over $\mathbb{F}_q$, given by

$$\theta^+(\sum_{i=1}^{2n} x_i e^i) = \sum_{i=1}^{n} x_i x_{n+i},$$

where
$\{e^1 = {}^t[10\ldots0], e^2 = {}^t[01\ldots0], \ldots, e^{2n} = {}^t[0\ldots01]\}$ is the standard basis of $\mathbb{F}_q^{2n\times 1}$.

The group $O^+(2n,q)$ of all isometries of $(\mathbb{F}_q^{2n\times 1}, \theta^+)$ is given by :

$$O^+(2n,q) = \left\{ \begin{bmatrix} A & B \\ C & D \end{bmatrix} \in GL(2n,q) \Big|^{{}^tAC, {}^tBD \text{ are alternating}}_{{}^tAD + {}^tCB = 1_n} \right\} = \left\{ \begin{bmatrix} A & B \\ C & D \end{bmatrix} \in GL(2n,q) \Big|^{{}^tAB, {}^tCD \text{ are alternating}}_{A^tD + B^tC = 1_n} \right\},$$

where A, B, C, D are of size n.

An $n \times n$ matrix $A = (a_{ij})$ over $\mathbb{F}_q$ is called alternating if

$$\begin{cases} a_{ii} = 0, & \text{for } 1 \leq i \leq n, \\ a_{ij} = -a_{ji} = a_{ji}, & \text{for } 1 \leq i < j \leq n. \end{cases}$$

$P^+ = P^+(2n,q)$ is the maximal parabolic subgroup of $O^+(2n,q)$ defined by:

$$P^+(2n,q) = \left\{ \begin{bmatrix} A & 0 \\ 0 & {}^tA^{-1} \end{bmatrix} \begin{bmatrix} 1_n & B \\ 0 & 1_n \end{bmatrix} \Big|^{A \in GL(n,q)}_{B \text{ alternating}} \right\}.$$

Then, with respect to $P^+ = P^+(2n,q)$, the Bruhat decomposition of $O^+(2n,q)$ is given by:

$$O^+(2n,q) = \coprod_{r=0}^{n} P^+ \sigma_r^+ P^+, \quad (9)$$

where

$$\sigma_r^+ = \begin{bmatrix} 0 & 0 & 1_r & 0 \\ 0 & 1_{n-r} & 0 & 0 \\ 1_r & 0 & 0 & 0 \\ 0 & 0 & 0 & 1_{n-r} \end{bmatrix} \in O^+(2n,q).$$

Put, for $0 \le r \le n$,

$$A_r^+ = \{w \in P^+(2n,q) \mid \sigma_r^+ w(\sigma_r^+)^{-1} \in P^+(2n,q)\}.$$

Expressing $O^+(2n,q)$ as a disjoint union of right cosets of $P^+ = P^+(2n,q)$, the Bruhat decomposition in (9) can be written as

$$O^+(2n,q) = \coprod_{r=0}^{n} P^+ \sigma_r^+ (A_r^+ \backslash P^+). \tag{10}$$

The order of the general linear group $GL(n,q)$ is given by

$$g_n = \prod_{j=0}^{n-1}(q^n - q^j) = q^{\binom{n}{2}} \prod_{j=1}^{n}(q^j - 1).$$

For integers n, r with $0 \le r \le n$, the q-binomial coefficients are defined as:

$$\begin{bmatrix} n \\ r \end{bmatrix}_q = \prod_{j=0}^{r-1}(q^{n-j}-1)/(q^{r-j}-1). \tag{11}$$

Then, for integers n, r with $0 \le r \le n$, we have

$$\frac{g_n}{g_{n-r} g_r} = q^{r(n-r)} \begin{bmatrix} n \\ r \end{bmatrix}_q. \tag{12}$$

As it is shown in [8],

$$\mid A_r^+ \mid = g_r g_{n-r} q^{\binom{n}{2}} q^{r(2n-3r+1)/2}. \tag{13}$$

Also, it is immediate to see that

$$\mid P^+(2n,q) \mid = q^{\binom{n}{2}} g_n. \tag{14}$$

Thus we get, from (12)-(14),

$$\mid A_r^+ \backslash P^+(2n,q) \mid = \begin{bmatrix} n \\ r \end{bmatrix}_q q^{\binom{r}{2}},$$

and

$$\mid P^+(2n,q) \mid^2 \mid A_r^+ \mid^{-1} = q^{\binom{n}{2}} g_n \begin{bmatrix} n \\ r \end{bmatrix}_q q^{\binom{r}{2}}. \tag{15}$$

So, from (10), (15), we get:

$$\begin{aligned} \mid O^+(2n,q) \mid &= \sum_{r=0}^{n} \mid P^+(2n,q) \mid^2 \mid A_r^+ \mid^{-1} \\ &= 2q^{n^2-n}(q^n - 1) \prod_{j=1}^{n-1}(q^{2j} - 1), \end{aligned} \tag{16}$$

where one can apply the following q-binomial theorem with $x = -1$.

$$\sum_{r=0}^{n} \begin{bmatrix} n \\ r \end{bmatrix}_q (-1)^r q^{\binom{r}{2}} x^r = (x;q)_n,$$

with $(x;q)_n = (1-x)(1-qx)\cdots(1-q^{n-1}x)$

(x an indeterminate, n a positive integer).

There is an epimorphism of groups $\delta^+ : O^+(2n,q) \to \mathbb{F}_2^+$($\mathbb{F}_2^+$ denoting the additive group of $\mathbb{F}_2$) , which is related to the Clifford algebra $C(\mathbb{F}_q^{2n\times 1}, \theta^+)$ of the quadratic space $(\mathbb{F}_q^{2n\times 1}, \theta^+)$, and is given by

$$\delta^+(w) = Tr(B\ {}^tC),$$

where

$$w = \begin{bmatrix} A & B \\ C & D \end{bmatrix} \in O^+(2n,q).$$

Then $SO^+(2n,q) := Ker\ \delta^+$ is given by

$$SO^+(2n,q) = \coprod_{0\le r\le n,\ r\ even} P^+ \sigma_r^+ (A_r^+ \backslash P^+), \tag{17}$$

and

$$\mid SO^+(2n,q) \mid \ = q^{n^2-n}(q^n - 1) \prod_{j=1}^{n-1}(q^{2j} - 1) (cf.\ (16)).$$

III. Gauss sums for $O^+(2n,q)$

The following notations will be used throughout this paper.

$tr(x) = x + x^2 + \cdots + x^{2^{r-1}}$ the trace function $\mathbb{F}_q \to \mathbb{F}_2$,

$\lambda(x) = (-1)^{tr(x)}$ the canonical additive character of $\mathbb{F}_q$.

Then any nontrivial additive character ψ of $\mathbb{F}_q$ is given by $\psi(x) = \lambda(ax)$, for a unique $a \in \mathbb{F}_q^*$.

For any nontrivial additive character ψ of $\mathbb{F}_q$ and $a \in \mathbb{F}_q^*$, the Kloosterman sum $K_{GL(t,q)}(\psi; a)$ for $GL(t,q)$ is defined as

$$K_{GL(t,q)}(\psi; a) = \sum_{w \in GL(t,q)} \psi(Trw + a\ Trw^{-1}). \tag{18}$$

Observe that, for $t = 1$, $K_{GL(1,q)}(\psi; a)$ denotes the Kloosterman sum $K(\psi; a)$.

For the Kloosterman sum $K(\psi; a)$, we have the Weil bound (cf. [11])

$$\mid K(\psi; a) \mid \le 2\sqrt{q}. \tag{19}$$

In [6], it is shown that $K_{GL(t,q)}(\psi; a)$ satisfies the following recursive relation: for integers $t \ge 2$, $a \in \mathbb{F}_q^*$,

$$\begin{aligned} K_{GL(t,q)}(\psi; a) &= q^{t-1} K_{GL(t-1,q)}(\psi; a) K(\psi; a) \\ &\quad + q^{2t-2}(q^{t-1} - 1) K_{GL(t-2,q)}(\psi; a), \end{aligned} \tag{20}$$

where we understand that $K_{GL(0,q)}(\psi; a) = 1$. From (20), in [6] an explicit expression of the Kloosterman sum for $GL(t,q)$ was derived.

Theorem 2 ([6]): For integers $t \ge 1$, and $a \in \mathbb{F}_q^*$, the Kloosterman sum $K_{GL(t,q)}(\psi; a)$ is given by

$$\begin{aligned} K_{GL(t,q)}(\psi; a) = q^{(t-2)(t+1)/2} &\sum_{l=1}^{[(t+2)/2]} q^l K(\psi; a)^{t+2-2l} \\ &\times \sum \prod_{\nu=1}^{l-1} (q^{j_\nu - 2\nu} - 1), \end{aligned} \tag{21}$$

where $K(\psi; a)$ is the Kloosterman sum and the inner sum is over all integers $j_1, \ldots, j_{l-1}$ satisfying $2l - 1 \le j_{l-1} \le j_{l-2} \le \cdots \le j_1 \le t + 1$. Here we agree that the inner sum is 1 for $l = 1$.

In Section 6 of [8], it is shown that the Gauss sums for $O^+(2n,q)$ and $SO^+(2n,q)$ are respectively given by:

$$\sum_{w\in O^+(2n,q)}\psi(Trw)=\sum_{r=0}^{n}|A_r^+\backslash P^+|\sum_{w\in P^+}\psi(Tr\ w\sigma_r^+)$$
$$=q^{\binom{n}{2}}\sum_{r=0}^{n}{\begin{bmatrix}n\\r\end{bmatrix}}_q q^{(2rn-r^2-r)/2}s_r \times K_{GL(n-r,q)}(\psi;1), \tag{22}$$

$$\sum_{w\in SO^+(2n,q)}\psi(Trw)=\sum_{\substack{0\le r\le n,\\ r\ even}}|A_r^+\backslash P^+|\sum_{w\in P^+}\psi(Tr\ w\sigma_r^+)$$
$$=q^{\binom{n}{2}}\sum_{\substack{0\le r\le n,\\ r\ even}}{\begin{bmatrix}n\\r\end{bmatrix}}_q q^{(2rn-r^2-r)/2}s_r \times K_{GL(n-r,q)}(\psi;1) \tag{23}$$

(cf. (10),(17)). Here ψ is any nontrivial additive character of $\mathbb{F}_q$, $s_0=1$, and, for $r\in\mathbb{Z}_{>0}$, s_r denotes the number of all $r\times r$ nonsingular symmetric matrices over $\mathbb{F}_q$, which is given by

$$s_r=\begin{cases} q^{r(r+2)/4}\prod_{j=1}^{r/2}(q^{2j-1}-1), & \text{for } r \text{ even},\\ q^{(r^2-1)/4}\prod_{j=1}^{(r+1)/2}(q^{2j-1}-1), & \text{for } r \text{ odd},\end{cases} \tag{24}$$

(cf. Proposition 4.3 in [8]).

For our purposes, we only need the following three expressions of the Gauss sums for $SO^+(2,q)$, $O^+(2,q)$, and $SO^+(4,q)$. So we state them separately as a theorem (cf. (11), (21)–(24)). Also, for the ease of notations, we introduce

$$G_1(q)=SO^+(2,q), G_2(q)=O^+(2,q), G_3(q)=SO^+(4,q). \tag{25}$$

Theorem 3: Let ψ be any nontrivial additive character of $\mathbb{F}_q$. Then we have

$$\sum_{w\in G_1(q)}\psi(Trw)=K(\psi;1),$$
$$\sum_{w\in G_2(q)}\psi(Trw)=K(\psi;1)+q-1,$$
$$\sum_{w\in G_3(q)}\psi(Trw)=q^2(K(\psi;1)^2+q^3-q).$$

For the following lemma, one notes that $(n,q-1)=1$.

Lemma 4: With $n=2^s(s\in\mathbb{Z}_{\ge 0})$, the map $a\mapsto a^n:\mathbb{F}_q^*\to\mathbb{F}_q^*$ is bijection.

A result analogous to the following Corollary is also mentioned in [15].

Corollary 5: For $n=2^s(s\in\mathbb{Z}_{\ge 0})$, and ψ a nontrivial additive character of $\mathbb{F}_q$,

$$K(\psi;a^n)=K(\psi;a).$$

Proof:

$$K(\psi;a^n)=\sum_{\alpha\in\mathbb{F}_q^*}\psi(\alpha+a^n\alpha^{-1})$$
$$=\sum_{\alpha\in\mathbb{F}_q^*}\psi(\alpha^n+a^n\alpha^{-n})\text{(by Lemma 4)}$$
$$=\sum_{\alpha\in\mathbb{F}_q^*}\psi((\alpha+a\alpha^{-1})^n)$$
$$=\sum_{\alpha\in\mathbb{F}_q^*}\psi(\alpha+a\alpha^{-1})([11],\text{Theorem 2.23(v)})$$
$$=K(\psi;a).$$

■

For the next corollary, we need a result of Carlitz.

Theorem 6 ([2]): For the canonical additive character λ of $\mathbb{F}_q$, and $a\in\mathbb{F}_q^*$,

$$K_2(\lambda;a)=K(\lambda;a)^2-q. \tag{26}$$

The next corollary follows from Theorems 3 and 6, Corollary 5, and by simple change of variables.

Corollary 7: Let λ be the canonical additive character of $\mathbb{F}_q$, and let $a\in\mathbb{F}_q^*$. Then we have

$$\sum_{w\in G_1(q)}\lambda(aTrw)=K(\lambda;a), \tag{27}$$
$$\sum_{w\in G_2(q)}\lambda(aTrw)=K(\lambda;a)+q-1, \tag{28}$$
$$\sum_{w\in G_3(q)}\lambda(aTrw)=q^2(K(\lambda;a)^2+q^3-q) \tag{29}$$
$$=q^2(K_2(\lambda;a)+q^3). \tag{30}$$

Proposition 8: Let λ be the canonical additive character of $\mathbb{F}_q$, $m\in\mathbb{Z}_{>0}$, $\beta\in\mathbb{F}_q$. Then

$$\sum_{a\in\mathbb{F}_q^*}\lambda(-a\beta)K_m(\lambda;a) = \begin{cases} qK_{m-1}(\lambda;\beta^{-1})+(-1)^{m+1}, & \text{if } \beta\neq 0,\\ (-1)^{m+1}, & \text{if } \beta=0,\end{cases} \tag{31}$$

with the convention $K_0(\lambda;\beta^{-1})=\lambda(\beta^{-1})$.

Proof: (31) is equal to

$$\sum_{\alpha_1,\dots,\alpha_m\in\mathbb{F}_q^*}\lambda(\alpha_1+\cdots+\alpha_m)\sum_{a\in\mathbb{F}_q^*}\lambda(a(\alpha_1^{-1}\cdots\alpha_m^{-1}-\beta))$$
$$=\sum_{\alpha_1,\dots,\alpha_m\in\mathbb{F}_q^*}\lambda(\alpha_1+\cdots+\alpha_m)\sum_{a\in\mathbb{F}_q}\lambda(a(\alpha_1^{-1}\cdots\alpha_m^{-1}-\beta)) - \sum_{\alpha_1,\dots,\alpha_m\in\mathbb{F}_q^*}\lambda(\alpha_1+\cdots+\alpha_m)$$
$$=q\sum\lambda(\alpha_1+\cdots+\alpha_m)+(-1)^{m+1}.$$

Here the sum runs over all $\alpha_1,\dots,\alpha_m\in\mathbb{F}_q^*$ satisfying $\alpha_1^{-1}\cdots\alpha_m^{-1}=\beta$, so that it is given by

$$\begin{cases} 0, & \text{if } \beta=0,\\ K_{m-1}(\lambda;\beta^{-1}), & \text{if } \beta\neq 0, \text{ and } m>1,\\ \lambda(\beta^{-1}), & \text{if } \beta\neq 0, \text{ and } \ m=1.\end{cases}$$

■

Let $G(q)$ be one of finite classical groups over $\mathbb{F}_q$. Then we put, for each $\beta \in \mathbb{F}_q$,

$$N_{G(q)}(\beta) = \mid \{w \in G(q) \mid Tr(w) = \beta\} \mid .$$

Then it is easy to see that

$$qN_{G(q)}(\beta) = \mid G(q) \mid + \sum_{a \in \mathbb{F}_q^*} \lambda(-a\beta) \sum_{w \in G(q)} \lambda(a\, Trw). \quad (32)$$

For brevity, we write

$$n_1(\beta) = N_{G_1(q)}(\beta), n_2(\beta) = N_{G_2(q)}(\beta), n_3(\beta) = N_{G_3(q)}(\beta). \quad (33)$$

Using (27), (28), (30)–(32), and (37), one derives the following.

Proposition 9: With $n_1(\beta), n_2(\beta), n_3(\beta)$ as in (33), we have

$$n_1(\beta) = \begin{cases} 1, & \text{if } \beta = 0, \\ 2, & \text{if } \beta \neq 0 \text{ with } tr(\beta^{-1}) = 0, \\ 0, & \text{if } \beta \neq 0 \text{ with } tr(\beta^{-1}) = 1, \end{cases} \quad (34)$$

$$n_2(\beta) = \begin{cases} q, & \text{if } \beta = 0, \\ 2, & \text{if } \beta \neq 0 \text{ with } tr(\beta^{-1}) = 0, \\ 0, & \text{if } \beta \neq 0 \text{ with } tr(\beta^{-1}) = 1, \end{cases} \quad (35)$$

$$n_3(\beta) = \begin{cases} q^3(2q^2 - q - 2), & \text{if } \beta = 0, \\ q^2\{q(q+1)(q-2) + K(\lambda; \beta^{-1})\}, & \text{if } \beta \neq 0. \end{cases} \quad (36)$$

IV. Construction of codes

Let

$$N_1 = |G_1(q)| = q - 1, N_2 = |G_2(q)| = 2(q-1), \\ N_3 = |G_3(q)| = q^2(q^2-1)^2. \quad (37)$$

Here we will construct three binary linear codes $C(G_1(q))$ of length N_1, $C(G_2(q))$ of length N_2 , and $C(G_3(q))$ of length N_3, respectively associated with the orthogonal groups $G_1(q)$,$G_2(q)$, and $G_3(q)$.

By abuse of notations, for $i = 1, 2, 3$, let $g_1, g_2, \ldots, g_{N_i}$ be a fixed ordering of the elements in the group $G_i(q)$. Also, for $i = 1, 2, 3$, we put

$$v_i = (Trg_1, Trg_2, \ldots, Trg_{N_i}) \in \mathbb{F}_q^{N_i}.$$

Then, for $i = 1, 2, 3$, the binary linear code $C(G_i(q))$ is defined as

$$C(G_i(q)) = \{u \in \mathbb{F}_2^{N_i} \mid u \cdot v_i = 0\}, \quad (38)$$

where the dot denotes the usual inner product in $\mathbb{F}_q^{N_i}$.

The following Delsarte's theorem is well-known.

Theorem 10 ([12]): Let B be a linear code over $\mathbb{F}_q$. Then

$$(B|_{\mathbb{F}_2})^{\perp} = tr(B^{\perp}).$$

In view of this theorem, the dual $C(G_i(q))^{\perp} (i = 1, 2, 3)$ is given by

$$C(G_i(q))^{\perp} = \{c(a) = (tr(aTrg_1), \ldots, tr(aTrg_{N_i})) | a \in \mathbb{F}_q\}. \quad (39)$$

Let $\mathbb{F}_2^+, \mathbb{F}_q^+$ denote the additive groups of the fields $\mathbb{F}_2, \mathbb{F}_q$, respectively. Then, with $\Theta(x) = x^2 + x$ denoting the Artin-Schreier operator in characteristic two, we have the following exact sequence of groups:

$$0 \to \mathbb{F}_2^+ \to \mathbb{F}_q^+ \to \Theta(\mathbb{F}_q) \to 0. \quad (40)$$

Here the first map is the inclusion and the second one is given by $x \mapsto \Theta(x) = x^2 + x$. So

$$\Theta(\mathbb{F}_q) = \{\alpha^2 + \alpha \mid \alpha \in \mathbb{F}_q\}, \ and \ \ [\mathbb{F}_q^+ : \Theta(\mathbb{F}_q)] = 2. \quad (41)$$

Theorem 11: Let λ be the canonical additive character of $\mathbb{F}_q$, and let $\beta \in \mathbb{F}_q^*$. Then

$$(a) \sum_{\alpha \in \mathbb{F}_q - \{0,1\}} \lambda(\frac{\beta}{\alpha^2 + \alpha}) = K(\lambda; \beta) - 1, \quad (42)$$

(b) $\sum_{\alpha \in \mathbb{F}_q} \lambda(\frac{\beta}{\alpha^2 + \alpha + a}) = -K(\lambda; \beta) - 1$, if $x^2 + x + a (a \in \mathbb{F}_q)$ is irreducible over $\mathbb{F}_q$, or equivalently if $a \in \mathbb{F}_q \setminus \Theta(\mathbb{F}_q)$ (cf.(41)).

Proof: (a) We compute the following sum in two different ways:

$$\sum_{a \in \mathbb{F}_q^*} \lambda(-\beta^{-1}a) K(\lambda; a)^2. \quad (43)$$

On the one hand, using (26) we see that (43) is equal to

$$\sum_{a \in \mathbb{F}_q^*} \lambda(-\beta^{-1}a)(q + K_2(\lambda; a)) \\ = -q + \sum_{a \in \mathbb{F}_q^*} \lambda(-\beta^{-1}a) K_2(\lambda; a) \quad (44) \\ = -q - 1 + qK(\lambda; \beta)(cf.(31)).$$

On the other hand, we see that (43) equals

$$\sum_{\alpha_1, \alpha_2 \in \mathbb{F}_q^*} \lambda(\alpha_1 + \alpha_2) \sum_{a \in \mathbb{F}_q^*} \lambda(a(\alpha_1^{-1} + \alpha_2^{-1} - \beta^{-1})) \\ = q \sum \lambda(\alpha_1 + \alpha_2) - 1$$

(with the sum running over all $\alpha_1, \alpha_2 \in \mathbb{F}_q^*$, satisfying $\alpha_1^{-1} + \alpha_2^{-1} = \beta^{-1}$)

$$= q \sum_{\alpha_1 \in \mathbb{F}_q - \{0, \beta\}} \lambda(\alpha_1 + (\alpha_1^{-1} + \beta^{-1})^{-1}) - 1 \\ = q \sum_{\alpha_1 \in \mathbb{F}_q - \{0, \beta^{-1}\}} \lambda(\alpha_1^{-1} + (\alpha_1 + \beta^{-1})^{-1}) - 1(\alpha_1 \to \alpha_1^{-1}) \\ = q \sum_{\alpha_1 \in \mathbb{F}_q - \{0,1\}} \lambda(\frac{\beta}{\alpha_1(\alpha_1 + 1)}) - 1(\alpha_1 \to \beta^{-1}\alpha_1). \quad (45)$$

Equating (44) and (45), the result (a) follows.

$$(b) \sum_{\alpha \in \mathbb{F}_q - \{0,1\}} \lambda(\frac{\beta}{\alpha^2 + \alpha}) = 2 \sum_{\gamma \in \Theta(\mathbb{F}_q) - \{0\}} \lambda(\frac{\beta}{\gamma}), \quad (46)$$

$$\sum_{\gamma \in \Theta(\mathbb{F}_q) - \{0\}} \lambda(\frac{\beta}{\gamma}) + \sum_{\gamma \in \Theta(\mathbb{F}_q)} \lambda(\frac{\beta}{\gamma + a}) = \sum_{\gamma \in \mathbb{F}_q^*} \lambda(\frac{\beta}{\gamma}) = -1. \quad (47)$$

So

$$\begin{aligned}\sum_{\alpha\in\mathbb{F}_q}\lambda(\frac{\beta}{\alpha^2+\alpha+a}) &= 2\sum_{\gamma\in\Theta(\mathbb{F}_q)}\lambda(\frac{\beta}{\gamma+a})(cf.(41))\\ &= -2-2\sum_{\gamma\in\Theta(\mathbb{F}_q)-\{0\}}\lambda(\frac{\beta}{\gamma})(cf.(47))\\ &= -2-\sum_{\alpha\in\mathbb{F}_q-\{0,1\}}\lambda(\frac{\beta}{\alpha^2+\alpha})(cf.(46))\\ &= -2-(K(\lambda;\beta)-1)(cf.(42))\\ &= -1-K(\lambda;\beta).\end{aligned}$$

■

Theorem 12: (a) For $q=2^r$, with $r\geq 3$, the map $\mathbb{F}_q\rightarrow C(G_i(q))^{\perp}(a\mapsto c(a))$, for $i=1,2$, is an $\mathbb{F}_2$-linear isomorphism.
(b) For any $q=2^r$, the map $\mathbb{F}_q\rightarrow C(G_3(q))^{\perp}(a\mapsto c(a))$ is an $\mathbb{F}_2$-linear isomorphism.

Proof: (a) As $G_2(q)=O^+(2,q)$ case can be shown in exactly the same manner, we will treat only $G_1(q)=SO^+(2,q)$ case. The map is clearly $\mathbb{F}_2$-linear and surjective. Let a be in the kernel of the map. Then $tr(aTrg)=0$, for all $g\in SO^+(2,q)$. Since $n_1(\beta)=|\{g\in SO^+(2,q)\mid Tr(g)=\beta\}|=2$, for all $\beta\in\mathbb{F}_q^*$ with $tr(\beta^{-1})=0$(cf. (34)), $tr(a\beta)=0$, for all $\beta\in\mathbb{F}_q^*$ with $tr(\beta^{-1})=0$. Hilbert's theorem 90 says that, for $\gamma\in\mathbb{F}_q$,$tr(\gamma)=0\Leftrightarrow\gamma=\alpha^2+\alpha$, for some $\alpha\in\mathbb{F}_q$. Thus $tr(\frac{a}{\alpha^2+\alpha})=0$, for all $\alpha\in\mathbb{F}_q\backslash\{0,1\}$. So $\sum_{\alpha\in\mathbb{F}_q-\{0,1\}}\lambda(\frac{a}{\alpha^2+\alpha})=q-2$. Assume now that $a\neq 0$. Then, from (42), (19),

$$q-2=K(\lambda;a)-1\leq 2\sqrt{q}-1$$

This implies that $q\leq 2\sqrt{q}+1$. But this is impossible, since $x>2\sqrt{x}+1$, for $x\geq 8$.
(b) Again, the map is $\mathbb{F}_2$-linear and surjective. From (36) and using the Weil bound in (19), it is elementary to see that $n_3(\beta)=|\{g\in SO^+(4,q)\mid Tr(g)=\beta)\}|>0$, for all $\beta\in\mathbb{F}_q$. Let a be in the kernel. Then $tr(aTrg)=0$, for all $g\in SO^+(4,q)$, and hence $tr(a\beta)=0$, for all $\beta\in\mathbb{F}_q$. This implies that $a=0$, since otherwise $tr:\mathbb{F}_q\rightarrow\mathbb{F}_2$ would be the trivial map. ■

Remark: It is easy to check that, for $i=1,2$, and $q=2^r$ with $r=1,2$, the kernel of the map $\mathbb{F}_q\rightarrow C(G_i(q))^{\perp}(a\mapsto c(a))$ is $\mathbb{F}_2$.

V. Power moments of Kloosterman sums

In this section, we will be able to find, via Pless power moment identity, a recursive formula for the power moments of Kloosterman sums in terms of the frequencies of weights in $C(G_i(q))$, for each $i=1,2,3$.

Theorem 13 (Pless power moment identity): Let B be an q-ary $[n,k]$ code, and let B_i (resp. $B_i^{\perp}$) denote the number of codewords of weight i in B(resp. in $B^{\perp}$). Then, for $h=0,1,2,\ldots,$

$$\begin{aligned}\sum_{j=0}^{n}j^hB_j=&\sum_{j=0}^{min\{n,h\}}(-1)^jB_j^{\perp}\\ &\times\sum_{t=j}^{h}t!S(h,t)q^{k-t}(q-1)^{t-j}\binom{n-j}{n-t},\end{aligned}\quad(48)$$

where $S(h,t)$ is the Stirling number of the second kind defined in (3).

From now on, we will assume that $r\geq 3$, for $i=1,2$, and hence, for $i=1,2,3$, every codeword in $C(G_i(q))^{\perp}$ can be written as $c(a)$, for a unique $a\in\mathbb{F}_q$(cf. Theorem 12, (39)). Further, we will assume $r\geq 2$, for $i=3$, so that Theorem 17 can be used in (c) of Theorem 18.

Lemma 14: Let $c(a)=(tr(aTrg_1),\cdots,tr(aTrg_{N_i}))\in C(G_i(q))^{\perp}$, for $a\in\mathbb{F}_q^*$, and $i=1,2,3$. Then the Hamming weight $w(c(a))$ can be expressed as follows:

$$(a)\ For\ i=1,2,\ w(c(a))=\frac{1}{2}(q-1-K(\lambda;a)),\quad(49)$$

$$\begin{aligned}(b)\ For\ i=3,\ &w(c(a))\\ &=\frac{1}{2}q^2(q^4-q^3-2q^2+q+1-K(\lambda;a)^2)\\ &=\frac{1}{2}q^2(q^4-q^3-2q^2+1-K_2(\lambda;a)).\end{aligned}\quad(50)$$

Proof:

$$\begin{aligned}For\ i=1,2,3,\ w(c(a))&=\frac{1}{2}\sum_{j=1}^{N_i}(1-(-1)^{tr(aTrg_j)})\\ &=\frac{1}{2}(N_i-\sum_{w\in G_i(q)}\lambda(aTrw)).\end{aligned}$$

Our results now follow from (37) and (27)-(30). ■

Fix $i(i=1,2,3)$, and let $u=(u_1,\ldots,u_{N_i})\in\mathbb{F}_2^{N_i}$, with ν_β 1's in the coordinate places where $Tr(g_j)=\beta$, for each $\beta\in\mathbb{F}_q$. Then we see from the definition of the code $C(G_i(q))$(cf. (38)) that u is a codeword with weight j if and only if $\sum_{\beta\in\mathbb{F}_q}\nu_\beta=j$ and $\sum_{\beta\in\mathbb{F}_q}\nu_\beta\beta=0$ (an identity in $\mathbb{F}_q$). As there are $\prod_{\beta\in\mathbb{F}_q}\binom{n_i(\beta)}{\nu_\beta}$ many such codewords with weight j, we obtain the following result.

Proposition 15: Let $\{C_{i,j}\}_{j=0}^{N_i}$ be the weight distribution of $C(G_i(q))$, for each $i=1,2,3$, where $C_{i,j}$denotes the frequency of the codewords with weight j in $C(G_i(q))$. Then

$$C_{i,j}=\sum\prod_{\beta\in\mathbb{F}_q}\binom{n_i(\beta)}{\nu_\beta},\quad(51)$$

where the sum runs over all the sets of integers $\{\nu_\beta\}_{\beta\in\mathbb{F}_q}(0\leq\nu_\beta\leq n_i(\beta))$, satisfying

$$\sum_{\beta\in\mathbb{F}_q}\nu_\beta=j,\ \text{and}\ \sum_{\beta\in\mathbb{F}_q}\nu_\beta\beta=0\quad(52)$$

Corollary 16: Let $\{C_{i,j}\}_{j=0}^{N_i}$ be the weight distribution of $C(G_i(q))$, for $i = 1, 2, 3$. Then, for $i = 1, 2, 3$, we have:

$$C_{i,j} = C_{i,N_i-j},$$

for all j, with $0 \le j \le N_i$.

Proof: Under the replacements $\nu_\beta \to n_i(\beta) - \nu_\beta$, for each $\beta \in \mathbb{F}_q$, the first equation in (52) is changed to $N_i - j$, while the second one in (52) and the summands in (51) are left unchanged. Here the second sum in (52) is left unchanged, since $\sum_{\beta \in \mathbb{F}_q} n_i(\beta)\beta = 0$, as one can see by using the explicit expressions of $n_i(\beta)$ in (34)–(36). ∎

Theorem 17 ([10]): Let $q = 2^r$, with $r \ge 2$. Then the range R of $K(\lambda; a)$, as a varies over $\mathbb{F}_q^*$, is given by:

$$R = \{t \in \mathbb{Z} \mid |t| < 2\sqrt{q}, t \equiv -1 (mod\ 4)\}.$$

In addition, each value $t \in R$ is attained exactly $H(t^2 - q)$ times, where $H(d)$ is the Kronecker class number of d.

Now, we get the following formulas in (2), (5), and (8), by applying the formula in (51) to each $C(G_i(q))$, using the explicit values of $n_i(\beta)$ in (34)-(36), and taking Theorem 17 into consideration.

Theorem 18: Let $\{C_{i,j}\}_{j=0}^{N_i}$ be the weight distribution of $C(G_i(q))$, for $i = 1, 2, 3$. Then

$$(a)\ C_{1,j} = \sum \binom{1}{\nu_0} \prod_{tr(\beta^{-1})=0} \binom{2}{\nu_\beta} (j = 0, \ldots, N_1),$$

where the sum is over all the sets of nonnegative integers $\{\nu_0\} \cup \{\nu_\beta\}_{tr(\beta^{-1})=0}$ satisfying $\nu_0 + \sum_{tr(\beta^{-1})=0} \nu_\beta = j$ and $\sum_{tr(\beta^{-1})=0} \nu_\beta \beta = 0$.

$$(b)\ C_{2,j} = \sum \binom{q}{\nu_0} \prod_{tr(\beta^{-1})=0} \binom{2}{\nu_\beta} (j = 0, \ldots, N_2),$$

where the sum is over all the sets of nonnegative integers $\{\nu_0\} \cup \{\nu_\beta\}_{tr(\beta^{-1})=0}$ satisfying $\nu_0 + \sum_{tr(\beta^{-1})=0} \nu_\beta = j$ and $\sum_{tr(\beta^{-1})=0} \nu_\beta \beta = 0$.

$$(c)\ C_{3,j} = \sum \binom{m_0}{\nu_0} \prod_{\substack{|t|<2\sqrt{q} \\ t \equiv -1 (4)}} \prod_{K(\lambda;\beta^{-1})=t} \binom{m_t}{\nu_\beta} (j = 0, \ldots, N_3),$$

where the sum is over all the sets of nonnegative integers $\{\nu_\beta\}_{\beta \in \mathbb{F}_q}$ satisfying $\sum_{\beta \in \mathbb{F}_q} \nu_\beta = j$ and $\sum_{\beta \in \mathbb{F}_q} \nu_\beta \beta = 0$,

$$m_0 = q^3(2q^2 - q - 2),$$

and

$$m_t = q^2(q^3 - q^2 - 2q + t),$$

for all integers t satisfying $|t| < 2\sqrt{q}$ and $t \equiv -1$ (mod 4).

We now apply the Pless power moment identity in (48) to each $C(G_i(q))^\perp$, for $i = 1, 2, 3$, in order to obtain the results in Theorem 1(cf. (1), (4), (6), (7)) about recursive formulas.

Then the left hand side of that identity in (48) is equal to

$$\sum_{a \in \mathbb{F}_q^*} w(c(a))^h, \tag{53}$$

with the $w(c(a))$ in each case given by (49), (50).

For $i = 1, 2$, (53) is

$$\begin{aligned} &\frac{1}{2^h} \sum_{a \in \mathbb{F}_q^*} (q - 1 - K(\lambda; a))^h \\ &= \frac{1}{2^h} \sum_{a \in \mathbb{F}_q^*} \sum_{l=0}^{h} (-1)^l \binom{h}{l} (q-1)^{h-l} K(\lambda; a)^l \\ &= \frac{1}{2^h} \sum_{l=0}^{h} (-1)^l \binom{h}{l} (q-1)^{h-l} M K^l. \end{aligned} \tag{54}$$

Similarly, for $i = 3$, (53) equals

$$(\frac{q^2}{2})^h \sum_{l=0}^{h} (-1)^l \binom{h}{l} (q^4 - q^3 - 2q^2 + q + 1)^{h-l} M K^{2l} \tag{55}$$

$$= (\frac{q^2}{2})^h \sum_{l=0}^{h} (-1)^l \binom{h}{l} (q^4 - q^3 - 2q^2 + 1)^{h-l} M K_2^l. \tag{56}$$

Note here that, in view of (26), obtaining power moments of 2-dimensional Kloosterman sums is equivalent to getting even power moments of Kloosterman sums. Also, one has to separate the term corresponding to $l = h$ in (54)-(56), and notes $dim_{\mathbb{F}_2} C(G_i) = r$.

VI. Remarks and Examples

The explicit computations about power moments of Kloosterman sums was begun with the paper [17] of Salié in 1931, where he showed, for any odd prime q,

$$MK^h = q^2 M_{h-1} - (q-1)^{h-1} + 2(-1)^{h-1} (h \ge 1). \tag{57}$$

However, this holds for any prime power $q = p^r (p$ a prime). Here $M_0 = 0$, and for $h \in \mathbb{Z}_{>0}$,

$$M_h = \mid \{(\alpha_1, \ldots, \alpha_h) \in (\mathbb{F}_q^*)^h \mid \sum_{j=1}^{h} \alpha_j = 1 = \sum_{j=1}^{h} \alpha_j^{-1}\} \mid .$$

For positive integers h, we let

$$A_h = \mid \{(\alpha_1, \ldots, \alpha_h) \in (\mathbb{F}_q^*)^h \mid \sum_{j=1}^{h} \alpha_j = 0 = \sum_{j=1}^{h} \alpha_j^{-1}\} \mid .$$

Then $(q-1)M_{h-1} = A_h$, for any $h \in \mathbb{Z}_{>0}$. So (57) can be rewritten as

$$MK^h = \frac{q^2}{q-1} A_h - (q-1)^{h-1} + 2(-1)^{h-1}. \tag{58}$$

Iwaniec [5] showed the expression (58) for any prime q. However, the proof given there works for any prime power q, without any restriction. Also, this is a special case of Theorem 1 in [3], as mentioned in Remark 2 there.

For $q = p$ any prime, MK^h was determined for $h \leq 4$(cf. [5], [17]).

$$MK^1 = 1, \quad MK^2 = p^2 - p - 1,$$
$$MK^3 = (\frac{-3}{p})p^2 + 2p + 1$$
$$\text{(with the understanding}(\frac{-3}{2}) = -1, (\frac{-3}{3}) = 0),$$
$$MK^4 = \begin{cases} 2p^3 - 3p^2 - 3p - 1, & p \geq 3; \\ 1, & p = 2. \end{cases}$$

Except [1] for $1 \leq h \leq 4$ and [16] for $h = 6$, not much progress had been made until Moisio succeeded in evaluating MK^h, for the other values of h with $h \leq 10$ over the finite fields of characteristic two in [13] (Similar results exist also over the finite fields of characteristic three (cf. [4], [14])), So we have now closed form formulas for $h \leq 10$.

His result was a breakthrough, but the way it was proved is too indirect, since the frequencies are expressed in terms of the Eichler Selberg trace formulas for the Hecke operators acting on certain spaces of cusp forms for $\Gamma_1(4)$. In addition, the power moments of Kloosterman sums are obtained only for $h \leq 10$ and not for any higher order moments. On the other hand, our formulas in (1) and (4) allow one, at least in principle, to compute moments of all orders for any given q.

In below, for small values of i, we compute, by using (1), (2), and MAGMA, the frequencies C_i of weights in $C(SO^+(2, 2^4))$ and $C(SO^+(2, 2^5))$, and the power moments MK^i of Kloosterman sums over $\mathbb{F}_{2^4}$ and $\mathbb{F}_{2^5}$. In particular, our results confirm those of Moisio's given in [13], when $q = 2^4$ and $q = 2^5$.

TABLE I
The weight distribution of $C(SO^+(2, 2^4))$

w	frequency	w	frequency	w	frequency	w	frequency
0	1	4	77	8	403	12	31
1	1	5	181	9	323	13	7
2	7	6	323	10	181	14	1
3	31	7	403	11	77	15	1

TABLE II
The power moments of Kloosterman sums over $\mathbb{F}_{2^4}$

i	MK^i	i	MK^i	i	MK^i
0	15	10	604249199	20	159966016268924111
1	1	11	3760049569	21	1115184421375168321
2	239	12	28661262671	22	7829178965854277039
3	289	13	188901585601	23	54689811340914235489
4	7631	14	1380879340079	24	383400882469952537231
5	22081	15	9373110103009	25	2680945149821576426881
6	300719	16	67076384888591	26	1878092114994051098711 9
7	1343329	17	462209786722561	27	1313949224351835245906529
8	13118351	18	3272087534565359	28	9201220847929255683359 51
9	72973441	19	22721501074479649	29	6439066453841188580322241

TABLE III
The weight distribution of $C(SO^+(2, 2^5))$

w	frequency	w	frequency	w	frequency	w	frequency
0	1	8	246325	16	9392163	24	81895
1	1	9	630725	17	8285955	25	23159
2	15	10	1385867	18	6446125	26	5369
3	135	11	2644947	19	4410805	27	945
4	945	12	4410805	20	2644947	28	135
5	5369	13	6446125	21	1385867	29	15
6	23159	14	8285955	22	630725	30	1
7	81895	15	9392163	23	246325	31	1

TABLE IV
The power moments of Kloosterman sums over $\mathbb{F}_{2^5}$

i	MK^i	i	MK^i	i	MK^i
0	31	10	44833141471	20	733937760431358760351
1	1	11	138050637121	21	68559453438399827241601
2	991	12	4621008512671	22	863461649242434978921 91
3	-959	13	222917404819 21	23	851252336789971927746241
4	63391	14	497555476630111	24	102495230953749246484185 91
5	-63359	15	3171377872090561	25	104764273348415132423811841
6	5102431	16	55381758830599711	26	122417000807114856330843363 1
7	-678719	17	423220459165032961	27	128195740310437210113659164 81
8	460435231	18	63185516353273123 51	28	146828974390583504114568758431
9	613044481	19	544617309801674256 01	29	156277475228271752782658007681

REFERENCES

[1] L. Carlitz, "Gauss sums over finite fields of order 2^n," Acta Arith.,vol. 15 , pp. 247-265, 1969.

[2] L. Carlitz, "A note on exponential sums," Pacific J. Math.,vol. 30 , pp. 35-37, 1969.

[3] Hi-joon Chae and D. S. Kim, "A generalization of power moments of Kloosterman sums," Arch. Math.(Basel), vol. 89 , pp. 152-156, 2007.

[4] G. van der Geer, R. Schoof and M. van der Vlugt, "Weight formulas for ternary Melas codes," Math. Comp., vol. 58 , pp. 781-792, 1992.

[5] H. Iwaniec, "Topics in Classical Automorphic Forms," Amer. Math. Soc., Providence, R. I., 1997.

[6] D. S. Kim, "Gauss sums for symplectic groups over a finite field," Mh.Math., vol.126, pp. 55-71, 1998.

[7] D. S. Kim, "Codes associated with special linear groups and power moments of multi-dimensional Kloosterman sums," preprint(2008), arXiv:0807.3991v1 [math.NT].

[8] D. S. Kim and Y. H. Park, "Gauss sums for orthogonal groups over a finite field of characteristic two," Acta Arith., vol. 82, pp. 331-357, 1997.

[9] H. D. Kloosterman, "On the representation of numbers in the form $ax^2 + by^2 + cz^2 + dt^2$," Acta. Math. vol. 49 , pp. 407-464, 1926.

[10] G. Lachaud and J. Wolfmann, "The weights of the orthogonals of the extended quadratic binary Goppa codes," IEEE Trans. Inform. Theory, vol. 36 , pp. 686-692, 1990.

[11] R. Lidl and H. Niederreiter, *Finite Fields, 2nd ed.* Cambridge, U. K.:Cambridge University Pless, 1997, vol. 20, Encyclopedia of Mathematics and Its Applications.

[12] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error Correcting Codes.* Amsterdam, The Netherlands: North-Holland, 1998.

[13] M. Moisio, "The moments of a Kloosterman sum and the weight distribution of a Zetterberg-type binary cyclic code," IEEE Trans. Inform. Theory, vol. 53, pp. 843-847, 2007.

[14] M. Moisio, "On the moments of Kloosterman sums and fibre products of Kloosterman curves," Finite Fields Appl., vol.14, pp. 515-531, 2008.

[15] M. Moisio, "Kloosterman sums, elliptic curves, and irreducible polynomials with prescribed trace and norm," *Acta Arith., to appear.*

[16] M. Moisio and K. Ranto, "Kloosterman sum identities and low-weight codewords in a cyclic code with two zeros," Finite Fields Appl., vol.13, pp. 922-935, 2007.

[17] H. Salié, "Uber die Kloostermanschen Summen $S(u, v; q)$," Math. Z., vol. 34, pp. 91-109, 1931.

[18] R. Schoof and M. van der Vlugt, "Hecke operators and the weight distributions of certain codes," J. Combin. Theory Ser. A, vol. 57, pp.163-186, 1991.
[19] Z.-X. Wan, "Geometry of Classical Groups over Finite Fields," Studentlitteratur, Lund, 1993.